UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/874,258	06/06/2001	Victor Larson	00479.00032	5950

22907 7590 02/24/2005

BANNER & WITCOFF
1001 G STREET N W
SUITE 1100
WASHINGTON, DC 20001

EXAMINER	
PHUNKULH, BOB A	
ART UNIT	**PAPER NUMBER**
2661	

DATE MAILED: 02/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/874,258	LARSON, VICTOR	
	Examiner	Art Unit	
	Bob A. Phunkulh	2661	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-82* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-82* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *1/31/01; 7/9/2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 46-50, 56-59 are rejected under 35 U.S.C. 102(e) as being anticipated by Howard et al. (US 6353886), hereinafter Howard.

Regarding claim 46, Howard discloses a virtual private network (VPN) device, comprising:

a memory containing a certificate that has been signed by a certification authority, the signed certificate containing at least one VPN parameter for the VPN device that has been verified by the certification authority (the database 32 stores the certificates, see figure 3-4); and

a processor receiving a request for establishing a VPN and responds to the request by sending the signed certificate over a telecommunications network to a second VPN device based on the received request (the processor (not shown) receive user request and verified the certificate and allow the communication, see figure 4).

Regarding claim 47, Howard discloses the request is received from the second VPN device, and a signed certificate for the second VPN device, the signed certificate for the second VPN device containing at least one VPN parameter for the second VPN device that has been verified by a certification authority (verify attribute certificate, see figure 4).

Regarding claim 48, Howard discloses the processor verifies the signed certificate for the second VPN device before sending the signed certificate to the second VPN device (see figure 4).

Regarding claim 49, Howard discloses the processor verifies the signed certificate for the second VPN device using a public key associated with the second VPN device (see figure 4 and claim 1).

Regarding claim 50, Howard discloses the processor establishes a VPN based on each verified VPN parameter for the VPN device and based each verified VPN parameter for the second VPN device (see figure 4 and claim 1).

55. The VPN device according to claim 46, wherein the processor determines whether a policy rule contained in the memory prevents a VPN connection to the second VPN device; and wherein the processor sends the certificate to the second VPN device when no policy rule contained in the memory prevents a VPN connection to the second VPN device.

Regarding claim 56, Howard discloses the telecommunications network is the Internet (network 1, see figures 1 and 3).

Regarding claim 57, Howard discloses the request for establishing a VPN is a request for establishing a standing VPN connection (see figure 4).

Regarding claim 58, Howard discloses the request for establishing a VPN is a request for establishing a VPN of opportunity (see figure 1).

Regarding claim 59, Howard discloses the VPN device is one of a VPN concentrator, a router, a firewall and a host computer (see figure 3).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 4-7, 13-16, 21-23, 60, 63-65, 72-74, are rejected under 35 U.S.C. 103(a) as being unpatentable over Genty et al. (US 6,675,225), hereinafter Genty.

Regarding claim 1, Genty discloses a method for creating a VPN tunnel over a public Internet. The VPN channel between two end points over the Internet uses the assigned certificates (see col. 6 lines 35-51).

Genty fails to explicitly disclose exchanging the certificates between the first VPN device and the second VPN device.

However, it would have been obvious to one having ordinary skill in the art at the time of invention was made to exchanges the assigned certificates between the first VPN device and the second VPN device in order to positively authenticate either end of the communication link before data is transferred.

Regarding claim 4, Genty discloses receiving for establishing the VPN from a client device (client D 402, figure 4) that is associated with the first VPN (network 406, figure 4).

Regarding claim 5, Genty discloses the request includes a destination for the VPN (receive network 414, see figure 4).

Regarding claim 6, Genty discloses the request includes a source/destination designation for the VPN (sender and receiver, see figures 4-5).

Regarding claim 7, Genty fails to disclose the destination designation includes a wild card designation. However, it would have been obvious to one having ordinary skill in the art at the time of invention was made to designate the wild card destination just incase the designated receiver or destination is unable to receive the data at present time and forwarding the received data to it intended destination when available to

receive the data –thus minimizing the network resources by releasing the connection once the data has been deliver to the wild card destination or the intended destination.

Regarding claim 13, Genty discloses the network is the Internet (see figures 4-5).

Regarding claim 14, Genty discloses establishing the VPN between the first and second VPN devices establishes a standing VPN connection (secure VPN connection 420, see figure 4).

Regarding claim 15, Genty discloses establishing the VPN between the first and second VPN devices establishes a VPN of opportunity (secure VPN connection 420, see figure 4).

Regarding claim 16, Genty discloses a method for creating a VPN tunnel over a public Internet. The VPN channel between two end points over the Internet uses the assigned certificates (see col. 6 lines 35-51).

Genty fails to explicitly disclose exchanging the certificates between the first VPN device and the second VPN device.

However, it would have been obvious to one having ordinary skill in the art at the time of invention was made to exchanges the assigned certificates between the first VPN device and the second VPN device in order to positively authenticate either end of the communication link before data is transferred.

Regarding claim 21, Genty discloses the network is the Internet (see figures 4-5).

Regarding claim 22, Genty discloses establishing the VPN between the first and second VPN devices establishes a standing VPN connection (secure VPN connection 420, see figure 4).

Regarding claim 23, Genty discloses establishing the VPN between the first and second VPN devices establishes a VPN of opportunity (secure VPN connection 420, see figure 4).

Regarding claim 60, Genty discloses a computer-readable medium for creating a VPN tunnel over a public Internet. The VPN channel between two end points over the Internet uses the assigned certificates (see col. 6 lines 35-51).

Genty fails to explicitly disclose exchanging the certificates between the first VPN device and the second VPN device.

However, it would have been obvious to one having ordinary skill in the art at the time of invention was made to exchanges the assigned certificates between the first VPN device and the second VPN device in order to positively authenticate either end of the communication link before data is transferred.

Regarding claim 63, Genty discloses receiving for establishing the VPN from a client device (client D 402, figure 4) that is associated with the first VPN (network 406, figure 4).

Regarding claim 64, Genty discloses the request includes a destination for the VPN (receive network 414, see figure 4).

Regarding claim 65, Genty discloses the request includes a source/destination designation for the VPN (sender and receiver, see figures 4-5).

Regarding claim 72, Genty discloses the network is the Internet (see figure 4-5).

Regarding claim 73, Genty discloses establishing the VPN between the first and second VPN devices establishes a standing VPN connection (secure VPN connection 420, see figure 4).

Regarding claim 74, Genty discloses establishing the VPN between the first and second VPN devices establishes a VPN of opportunity (secure VPN connection 420, see figure 4).

Claims 2-3, 8-12, 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Genty in view of Howard.

Regarding claims 2-3, 8-12, 17-20 Genty is silent on sending a request to on-line database for obtaining a public key from either the sender or the receiver and determining whether a policy rule prevents a VPN connection to the VPN device.

Howard, on the other hand, discloses sending a request to on-line database for obtaining a public key from either the sender or the receiver (see claim 1 and figure 4).

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to includes the teaching of Howard in the system taught by Genty for providing a high degree of flexibility, and a broad range of network features, while maintaining high level of security in a VPN environment.

Claims 24-33, 36-39, 41-46, 75-82 are rejected under 35 U.S.C. 103(a) as being unpatentable over Genty in view of Muniyappa et al. (US 6,092,200), hereinafter Muniyappa.

Regarding claims 24, 27, 36-39, 41, Genty discloses a method for creating a VPN tunnel over a public Internet. The VPN channel between two end points over the Internet uses the assigned certificates (see col. 6 lines 35-51).

Genty fails to explicitly disclose sending a certificate request for the VPN device to a certification authority.

Muniyappa, on the other hand, discloses sending a certificate request for the VPN device to a certification authority before setting up the VPN link (see figure 1 and col. 5 lines 51-63).

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to provides the teaching of Muniyappa in the system taught by Genty in order to provides a secure communication tunnel over the public network thus the first VPN device and the second VPN device can positively authenticate either end of the communication link before data is transferred.

Regarding claim 25, Muniyappa discloses the certificate request includes at least one telecommunications network address (master node address information) that the VPN device will use for establishing a VPN device (see col. 5 lines 51-63).

Regarding claim 26, Muniyappa discloses the certificate request includes a range of telecommunications network addresses (the master node address information) that the VPN device will use for VPNs established through the VPN device (see col. 5 lines 51-63).

Regarding claim 28 Genty discloses the step of establishing the VPN is further based on a source and destination name pair (see figures 4-5).

Regarding claim 29, Genty- Muniyappa fail to disclose the destination designation includes a wild card designation. However, it would have been obvious to one having ordinary skill in the art at the time of invention was made to designate the wild card destination just incase the designated receiver or destination is unable to

receive the data at present time and forwarding the received data to it intended destination when available to receive the data –thus minimizing the network resources by releasing the connection once the data has been deliver to the wild card destination or the intended destination.

Regarding claim 30, Muniyappa discloses the step of establishing the VPN is further based on at least one rule allowing a VPN connection to the selected telecommunications network address (master node address information, see col. 5 lines 51-63).

Regarding claim 31-32, Genty discloses establishing the VPN based on QOS or bandwidth limitation parameter (see col. 6 lines 30-32).

Regarding claim 33, Genty discloses the telecommunications network is the Internet (see figures 4-5).

Regarding claim 42, Genty discloses a method for creating a VPN tunnel over a public Internet. The VPN channel between two end points over the Internet uses the assigned certificates (see col. 6 lines 35-51).

Genty fails to explicitly disclose sending a certificate request for the VPN device to a certification authority.

Muniyappa, on the other hand, discloses sending a certificate request for the VPN device to a certification authority before setting up the VPN link (see figure 1 and col. 5 lines 51-63).

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to provides the teaching of Muniyappa in the system taught by Genty in order to provides a secure communication tunnel over the public network thus the first VPN device and the second VPN device can positively authenticate either end of the communication link before data is transferred.

Regarding claim 43, Muniyappa discloses the certificate request includes at least one telecommunications network address (master node address information) that the VPN device will use for establishing a VPN, and wherein the step of verifying verifies each telecommunication network address contained in the certificate request (see col. 5 lines 51-63).

Regarding claim 44, Muniyappa discloses the certificate request includes a range of telecommunications network addresses (the master node address information) that the VPN device will use for VPNs established through the VPN device, and wherein the step of verifying verifies the range of telecommunications network addresses contained in the certificate request (see col. 5 lines 51-63).

Regarding claim 45, Genty discloses the telecommunications network is the Internet (see figures 4-5).

Regarding claim 46, Genty discloses a method for creating a VPN tunnel over a public Internet. The VPN channel between two end points over the Internet uses the assigned certificates (see col. 6 lines 35-51).

Genty fails to explicitly disclose sending a certificate request for the VPN device to a certification authority.

Muniyappa, on the other hand, discloses sending a certificate request for the VPN device to a certification authority before setting up the VPN link (see figure 1 and col. 5 lines 51-63).

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to provides the teaching of Muniyappa in the system taught by Genty in order to provides a secure communication tunnel over the public network thus the first VPN device and the second VPN device can positively authenticate either end of the communication link before data is transferred.

Regarding claim 75, Genty discloses a method for creating a VPN tunnel over a public Internet. The VPN channel between two end points over the Internet uses the assigned certificates (see col. 6 lines 35-51).

Genty fails to explicitly disclose sending a certificate request for the VPN device to a certification authority.

Muniyappa, on the other hand, discloses sending a certificate request for the VPN device to a certification authority before setting up the VPN link (see figure 1 and col. 5 lines 51-63).

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to provides the teaching of Muniyappa in the system taught by Genty in order to provides a secure communication tunnel over the public network thus the first VPN device and the second VPN device can positively authenticate either end of the communication link before data is transferred.

Regarding claim 76, Muniyappa discloses the certificate request includes at least one telecommunications network address (master node address information) that the VPN device will use for establishing a VPN, and wherein the step of verifying verifies each telecommunication network address contained in the certificate request (see col. 5 lines 51-63).

Regarding claim 77, Muniyappa discloses the certificate request includes a range of telecommunications network addresses (the master node address information) that the VPN device will use for VPNs established through the VPN device, and wherein the step of verifying verifies the range of telecommunications network addresses contained in the certificate request (see col. 5 lines 51-63).

Regarding claim 78, Genty discloses the telecommunications network is the Internet (see figures 4-5).

Regarding claim 79, Genty discloses a method for creating a VPN tunnel over a public Internet. The VPN channel between two end points over the Internet uses the assigned certificates (see col. 6 lines 35-51).

Genty fails to explicitly disclose sending a certificate request for the VPN device to a certification authority.

Muniyappa, on the other hand, discloses sending a certificate request for the VPN device to a certification authority before setting up the VPN link (see figure 1 and col. 5 lines 51-63).

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to provides the teaching of Muniyappa in the system taught by Genty in order to provides a secure communication tunnel over the public network thus the first VPN device and the second VPN device can positively authenticate either end of the communication link before data is transferred.

Regarding claim 80, Muniyappa discloses the certificate request includes at least one telecommunications network address (master node address information) that the VPN device will use for establishing a VPN, and wherein the step of verifying verifies each telecommunication network address contained in the certificate request (see col. 5 lines 51-63).

Regarding claim 81, Muniyappa discloses the certificate request includes a range of telecommunications network addresses (the master node address information) that the VPN device will use for VPNs established through the VPN device, and wherein the step of verifying verifies the range of telecommunications network addresses contained in the certificate request (see col. 5 lines 51-63).

Regarding claim 82, Genty discloses the telecommunications network is the Internet (see figures 4-5).

Claims 34-35, 40, 51-55 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Genty- Muniyappa as applied to claim 24 above, and further in view of Howard.

Regarding claim 34-35, 40, 51, 55 Genty is silent on sending a request to on-line database for obtaining a public key from either the sender or the receiver and determining whether a policy rule prevents a VPN connection to the VPN device.

Howard, on the other hand, discloses sending a request to on-line database for obtaining a public key from either the sender or the receiver (see claim 1 and figure 4).

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to includes the teaching of Howard in the system taught

by Genty for providing a high degree of flexibility, and a broad range of network features, while maintaining high level of security in a VPN environment.

Regarding claim 52, Genty discloses the request includes a destination for the VPN (receive network 414, see figure 4).

Regarding claim 53, Genty discloses the request includes a source/destination designation for the VPN (sender and receiver, see figures 4-5).

Regarding claim 54, the combination of Genty- Muniyappa-Howard fail to disclose the destination designation includes a wild card designation. However, it would have been obvious to one having ordinary skill in the art at the time of invention was made to designate the wild card destination just incase the designated receiver or destination is unable to receive the data at present time and forwarding the received data to it intended destination when available to receive the data –thus minimizing the network resources by releasing the connection once the data has been deliver to the wild card destination or the intended destination.

Claims 61-62, 64-71 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Genty in view of Howard.

Regarding claim 61-62, 67-71 Genty is silent on sending a request to on-line database for obtaining a public key from either the sender or the receiver and determining whether a policy rule prevents a VPN connection to the VPN device.

Howard, on the other hand, discloses sending a request to on-line database for obtaining a public key from either the sender or the receiver (see claim 1 and figure 4).

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to includes the teaching of Howard in the system taught by Genty for providing a high degree of flexibility, and a broad range of network features, while maintaining high level of security in a VPN environment.

Regarding claim 64, Genty discloses the request includes a destination for the VPN (receive network 414, see figure 4).

Regarding claim 65, Genty discloses the request includes a source/destination designation for the VPN (sender and receiver, see figures 4-5).

Regarding claim 66, Genty fails to disclose the destination designation includes a wild card designation. However, it would have been obvious to one having ordinary skill in the art at the time of invention was made to designate the wild card destination just incase the designated receiver or destination is unable to receive the data at present time and forwarding the received data to it intended destination when available to

receive the data –thus minimizing the network resources by releasing the connection once the data has been deliver to the wild card destination or the intended destination.

Conclusion

Any response to this action should be mailed to:

The following address mail to be delivered by the United States Postal Service (USPS) only:

Mail Stop _____
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

or faxed to:

(703) 872-9306, (for formal communications intended for entry)

Or:

The following address mail to be delivered by other delivery services (Federal Express (Fed Ex), UPS, DHL, Laser, Action, Purolater, Hand Delivery, etc.) as follow:

U.S. Patent and Trademark Office
220 20th Street South
Customer Window, Mail Stop _____
Crystal Plaza Two, Lobby, Room 1B03
Arlington, VA 22202.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Bob A. Phunkulh** whose telephone number is **(571) 272-3083.** The examiner can normally be reached on Monday-Tursday from 8:00 A.M.

to 5:00 P.M. (first week of the bi-week) and Monday-Friday (for second week of the bi-week).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor **Chau Nguyen**, can be reach on **(571) 272-3126.** The fax phone number for this group is **(703) 872-9306.**

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Bob A. Phunkulh

BOB PHUNKULH
PRIMARY EXAMINER

TC 2600
Art Unit 2661
February 22, 2005